

REMARKS

Applicant respectfully requests reconsideration of this application as amended. No claims have been amended. Claims 4, 10-16, 21-24 and 28 were cancelled without prejudice. No new claims have been added. Therefore, claims 1-3, 5-9, 17- 20, 25-27 and 39-30 are presented for examination.

35 U.S.C. § 103 Rejection

Claims 1-3, 5-9, 17-20, 25-27 and 29-30 stand rejected under 35 U.S.C. §103(a) as being anticipated over Matyas, Jr. et al., U.S. Patent No. 6,687,675 (“Matyas”) in view of Chen, et al., U.S. Patent No. 6,073,242 (“Chen”) and further in view of Hardy, et al., U.S. Patent No. 6,073,242 (“Hardy”) and further in view of Menezes, et al., “Handbook of Applied Cryptography” (“Menezes”).

Applicants respectfully disagree with the Examiner’s characterization of the references. Matyas discloses a “computer program which generate[s] a cryptographic key utilizing user specific information to generate a user dependent key.” (Abstract). Matyas further discloses “a PRNG . . . for generating pseudo random numbers. [T]he PRNG having only one secret seed value.” (col. 9, lines 19-25; emphasis provided).

Chen discloses “[a] method . . . for communicating encrypted user passwords from a client to a server.” (Abstract; emphasis provided). Chen further discloses that “[t]he server communicates to the client a server random seed value. The client then generates a client random seed value and, using both the client random seed value and the server random seed value, an encrypted user password. The client then communicates to the server the client random seed and the encrypted user password. Then the server validates the encrypted user password using both the server random seed and the client

random seed.” (col. 2, lines 1-9; emphasis provided).

Hardy discloses “[a]n electronic communication authority server that provides centralized key management, implementation of role-based enterprise policies and workflow and projection of corporate authorities over trusted networks.” (Abstract).

Hardy further discloses that “*a secure connection is a connection where the level of confidentiality, authentication, and integrity is sufficient for the purposes of the system owners and users.*” (col. 3, lines 54-56; emphasis provided).

Menezes discloses that “a session key is an ephemeral secret, i.e., one whose use is restricted to a short time period such as a single telecommunications connection, after which all trace of it is eliminated.” (page 494, lines 3-5).

The Examiner acknowledges that Matyas “fails to disclose securely obtaining additional seeding information from one or more remote entropy servers.” (Office Action, mailed 05/26/06, page 3; emphasis added) However, the Examiner asserts that Chen teaches the feature missing. Applicants disagree. Referring to the sections of Chen cited by the Examiner, Chen discloses “communicating encrypted user passwords from a client to a server. During new environment negotiations, the *server communicates to the client a server random seed value. The client then generates a client random seed value* and, using both the client random seed values and this server random seed value, an encrypted user password. The *client then communicates to the server the client random seed and the encrypted user password.* Then the user *validates the encrypted user password using both the server random seed and the client random seed.*” (col. 1, line 66 through col. 2, line 9; emphasis added). Nowhere does Chen disclose the feature of claim 1.

Furthermore, and importantly, the Examiner is referring only to partial elements of claim 1. For example, as discussed above, the Examiner refers to “securely obtaining additional seeding information from one or more remote entropy servers” of claim 1 as being disclosed by Chen. However, the element of claim 1 reads as “securely obtaining additional seeding information from one or more remote entropy servers using a secure entropy collection protocol, wherein the securely obtaining of the additional seeding information is repeated for each entropy server” (emphasis added). Applicants respectfully remind the Examiner that merely partial or even substantial disclosure of elements of the invention does not satisfy the requirements that every element of the claims is to be shown. Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987), Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Nevertheless, even when considering only the partial element of claim 1 as being considered by the Examiner, Chen does not make up for the deficiencies of Matyas. Also, Hardy and Menezes do not teach or reasonably disclose at least the above-referenced feature of claim 1. Hence, Matyas, Chen, Hardy and Manezes, neither individually nor when combined in any combination, teach or reasonably suggest at least the above-referenced element of claim 1. Accordingly, Applicants respectfully request the withdrawal of the rejection of claim 1 and its dependent claims.

Claims 17 and 25 contain limitations similar to those of claim 1. Accordingly, Applicants respectfully request the withdrawal of the rejection of claims 17 and 25 and their dependent claims

Conclusion

In light of the foregoing, reconsideration and allowance of the claims is hereby earnestly requested.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

Request for an Extension of Time

Applicant respectfully petitions for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17(a) for such an extension.


Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: August 23, 2006


Aslam A. Jaffery
Reg. No. 51,841

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1030
(303) 740-1980